

## Definition of data networks:

A data network is a collection of devices and circuits for transferring data from one computer to another. It enables users at different locations to share the resources of a computer stationed elsewhere.

## Definition of network management:

Due to the importance of a functioning data network, network engineers have responsibility of installing, maintaining, and troubleshooting the network. As networks grow in size, so do the size and number of potential problems and the scope of complexity of the network engineer's job. Engineers need to know large amounts of information about the data network. The sheer volume of this information can quickly become unmanageable.

To help network engineers do their jobs, the concept of network management evolved. The overall goal of network management is to help engineers deal with the complexity of a data network and to make sure that data can go across it with maximum efficiency and transparency to the user.

## The Network Management Platform

Management used to involve multiple systems each managing a specific set of components on the network e.g. hubs, bridges, routers, etc. Restrictions of money, physical space, and technical expertise all led to the desire to have the network components managed by a single system. Out of this need came the network management platform.

- GUI: gives the user easier access to the features of the platform.
- A network map: the map is useful for nearly every area of the network management. For example, fault management tools can isolate the cause of the fault, using colours on the map.
- A Database Management System: applications use the database for information storage. Relationships can be built between data items, which help in network diagnosis and maintenance.
- A standard method to query devices: this is essential because the platform must be able to gather information from many different vendor components.
- An event log: this log records each network event chronologically in a readable format. The platform writes information to the log about any known network events.
- A customisable menu system: is needed so that extensions to the platform appear seamless to the user.
- Graphing tools: this gives engineers the ability to produce graphs, such as line, or bar chart of data. Graphs of current network traffic and errors can help in fault and performance management.

- And API –Application Programming Interface: an API is a library of programming procedures and functions allowing access to information kept within the network management platform.
- System security: the network management platform and associated applications contain a wealth of information about the network. This information is useful for network crackers trying to compromise network security.

## Network Management Applications

The network management platform provides generic functionality for all managed devices. In contrast, the design of network management applications is the help manage a specific set of devices or services.

- Manage specific set of devices: For example, a switch manufacturer could build an application that shows the physical connectors on the hub when a user selects the switch on the network map. This application could allow the user to configure features of the switch, turn ports on or off, or monitor error rates and throughput.
- Avoid functionality overlap with the platform: overlap would result in multiple ways to accomplish the same result on the platform, perhaps providing a confusing interface for the user. Also it could be a waste of development effort.
- Integrate with the platform through the API and menu system: a network management application has the goal of interfacing with the platform to allow user to view the application and platform as one uniform network management system.
- Reside on multiple platforms: an application that is available only on a single platform forces the network engineer to use this platform. This is not an ideal situation because the single platform may not have the necessary features or support other needed applications.

This approach has one significant drawback: Applications do not share information.

## Network Management Architecture

A network management platform can use various architectures to provide functionality. There is no “best” architecture; each type has specific features that work well in certain environments.

**A centralised** architecture has the network management platform at one computer system, at a location that is responsible for all network management duties. This system uses a single centralised database that is backed up to another system at regular intervals.

### Advantages

- Network managers have a single location to view all network management information.
- Provides convenience, accessibility, and security for the network engineer.

## Disadvantages

- Having all of the network management functions depend on a single system is not fault tolerant.
- Full backups should be maintained.
- As the network grows in size, it may be difficult and expensive to scale a single system to handle the necessary load.
- Having to query all network devices from a single location puts traffic load on all network links connected to the management site and throughout the network.

## Hierarchical Architecture

### Advantages:

- Not dependent on a single system; no single point of failure
- Distribution of network management tasks; saving valuable bandwidth resources
- Network monitoring distributed throughout network
- Centralised data storage; many network management tasks require the retrieval of information about many aspects of the network. Therefore it is often beneficial to have a centralised location for data.

### Disadvantages:

- Still provide a single place to store information about the network
- It makes information gathering a bit more difficult and time consuming
- The list of devices managed by each client needs to be logically predetermined and manually configured

## Distributed Architecture

A replication service keeps multiple databases on different systems completely synchronised, not a trivial task.

## Network monitoring example:

### IFG:

Ethernet devices must allow a minimum idle period between transmission of Ethernet frames known as the interframe gap (IFG). A brief recovery time between frames allows devices to prepare for reception of the next frame. The minimum interframe gap is 96 bit times (the time it takes to transmit 96 bits of raw data on the medium), which is 9.6  $\mu$ s for 10 Mbit/s Ethernet, 960 ns for 100 Mbit/s (fast) Ethernet, 96 ns for 1 Gbit/s (gigabit) Ethernet, and 9.6 ns for 10 Gbit/s (10 gigabit) Ethernet.

### ICMP:

The Internet Control Message Protocol (ICMP) is one of the core protocols of the Internet Protocol Suite. It is chiefly used by networked computers' operating systems to send error messages—indicating, for instance, that a requested service is not available or that a host or router could not be reached.

ICMP [1] relies on IP to perform its tasks, and it is an integral part of IP. It differs in purpose from transport protocols such as TCP and UDP in that it is typically not used to send and receive data between end systems. It is usually not used directly by user network applications, with some notable exceptions being the ping tool and traceroute.